

WE CLAIM

1. A method of controlling a monitoring function of a processor, said processor being operable in at least two domains, comprising a first domain and a
5 second domain, said first and second domains each comprising at least one mode, said method comprising the steps of:

setting at least one control value, said at least one control value relating to a condition and being indicative of whether said monitoring function is allowable in said first domain; and

10 only allowing initiation of said monitoring function in said first domain when said condition is present if its related control value indicates that said monitoring function is allowable.

2. A method according to claim 1, wherein said first domain is a secure
15 domain and said second domain is a non-secure domain, said processor being operable such that when executing a program in a secure mode within said secure domain said program has access to secure data which is not accessible when said processor is operating in a non-secure mode within said non-secure domain.

20 3. A method according to claim 2, wherein said condition comprises a domain, mode or type of monitoring function.

4. A method according to claim 3, wherein said condition comprises a secure domain and said control value comprises a secure domain enable value,
25 initiation of monitoring in said secure domain only being allowed if said secure domain enable value is set.

5. A method according to claim 3, wherein said secure domain includes a secure user mode and said condition comprises a secure user mode.

6. A method according to claim 5 wherein said control value comprises a secure user mode enable bit and initiation of monitoring from secure user mode is only allowed if said secure user mode enable bit has been set.

5 7. A method according to claim 4, wherein said condition comprises a type of monitoring function.

8. A method according to claim 7, wherein said condition comprises a debug monitoring function and said control value comprises a debug enable bit,
10 initiation of debug in said first domain only being allowable if said debug enable bit has been set.

9. A method according to claim 8, wherein said condition comprises a trace monitoring function and said control value comprises a trace enable bit, initiation
15 of trace in said first domain only being allowable if said control trace enable bit has been set.

10. A method according to claim 9, wherein said secure domain enable value comprises a secure debug enable bit and a secure trace enable bit, initiation of
20 debug and trace in said secure domain only being allowable if respective portions of said secure domain enable value are set.

11. A method according to claim 1, said method comprising setting a plurality of control values, each of said plurality of control values relating to a
25 different condition; and

only allowing initiation of said monitoring function in said first domain if any of said conditions are present if each of said control values related to a condition that is present indicate that said monitoring function is allowable.

30 12. A method according to claim 1, said method further comprising said steps of:

setting a control indicator, said control indicator indicating that monitoring is only allowable for specified applications; and

prior to initialising said monitoring function checking an application identifier; and

5 only allowing initiation of said monitoring function if said application currently running is one for which monitoring is allowable.

13. A method according to claim 12, wherein the step of setting a control
10 indicator comprises setting a control indicator stored in a predetermined position in a storage element.

14. A method according to claim 12, wherein said monitoring function comprises monitoring said processor and capturing diagnostic data, said method
15 comprising the further step of:

following initiation of said monitoring function only allowing capturing of diagnostic data in said first domain while an application running on said processor is one for which monitoring is allowable.

20 15. A method according to claim 1, wherein said monitoring function comprises monitoring said processor and capturing diagnostic data, said method comprising the further step of:

25 following initiation of said monitoring function only allowing capturing of diagnostic data in said first domain when a condition changes if a control value related to the changed condition indicates that said monitoring function is allowable.

16. A method according to claim 1, wherein setting of at least one control value is performed either by setting said control value via an input port or by setting said control value from the first domain.

30

17. A method according to claim 16, said method comprising the further step of blocking write access to said control value via said input port such that the step

of setting said control value can henceforth only be performed by setting said control value from said first domain.

18. A method according to claim 1, wherein said first domain comprises a
5 first user mode and a first privileged mode and the step of setting at least one control value in said first domain, comprises setting said control value from said first privileged mode.

19. A method according to claim 16, wherein said first domain comprises a
10 first user mode and a first privileged mode and said step of setting at least one control value in the first domain, comprises inputting an authentication code from a mode that is not a first privileged mode and then setting said control value.

20. A processor operable in a first domain and a second domain said first
15 and second domains each comprising at least one mode, said processor comprising:
monitoring logic;

a storage element operable to be set to contain at least one control value, said at least one control value relating to a condition and being indicative of whether operation of said monitoring logic is allowable in said first domain; and

20 control logic operable to control initiation of said monitoring logic and only to allow initiation of said monitoring logic in said first domain when said condition is present if its related control value indicates that operation of said monitoring logic is allowable.

25 21. A processor according to claim 20, wherein said first domain is a secure domain and said second domain is a non-secure domain said processor being operable such that when executing a program in a secure mode within said secure domain said program has access to secure data which is not accessible when said processor is operating in a non-secure mode within said non-secure domain.

30

22. A processor according to claim 21, wherein said condition comprises a domain, mode or type of monitoring logic.

23. A processor according to claim 22, wherein said condition comprises a secure domain and said control value comprises a secure domain enable bit, initiation of monitoring in said secure domain only being allowed if said storage element
5 contains a secure domain enable bit.

24. A processor according to claim 22, wherein said secure domain includes a secure user mode and said condition comprises a secure user mode.

10 25. A processor according to claim 24 wherein said control value comprises a secure user mode enable bit and said control logic is operable to allow initiation of said monitoring logic from secure user mode only when said storage element contains a secure user mode enable bit.

15 26. A processor according to claim 21, wherein said condition comprises a type of monitoring function.

27. A processor according to claim 26, wherein said condition comprises debug monitoring and the control value comprises a debug enable bit, said control
20 logic being operable to allow initiation of said monitoring logic in said first domain only when the storage element contains a debug enable bit.

28. A processor according to claim 26, wherein said condition comprises trace monitoring and said control value comprises a trace enable bit, said control logic
25 being operable to allow initiation of said trace logic in said first domain only when said storage element contains a control trace enable bit.

29. A processor according to claim 20, wherein:
said storage element is operable to contain a plurality of control values, each of said
30 plurality of control values relating to a different condition; and

said control logic is operable to only allow initiation of said monitoring logic in said first domain if any of said conditions are present if each of the control values related to a condition that is present indicate that the monitoring logic is allowable.

5 30. A processor according to claim 29 wherein one condition comprises a secure domain and a corresponding control value comprises a secure domain enable bit and a further condition comprises a secure user mode and a corresponding control value comprises a secure user mode enable bit, said control logic being operable to initiate said monitoring logic from secure user mode only when said storage element
10 contains both a secure user mode enable bit and a secure domain enable bit.

31. A processor according to claim 20, wherein:
said storage element is further operable to contain a control indicator, said control indicator indicating that monitoring is only allowable for identified applications; and
15 said control logic is operable to check at least one identifier identifying an application that is allowable, said control logic only initiating said monitoring logic in the first domain when said application currently running is one identified as being one for which monitoring is allowable.

20 32. A processor according to claim 31, said processor comprising a further storage element, said storage element being operable to contain said at least one identifier specifying an application that is allowable.

25 33. A processor according to claim 31, wherein said monitoring logic is operable to monitor the processor and capture diagnostic data; and
wherein said control logic is operable to control the monitoring logic to suppress capturing of diagnostic data in said first domain when said control logic detects that said application running is not one identified as being allowable.

30 34. A processor according to claim 20, said processor further comprising an input port, wherein said control value is operable to be set in said storage element either via the input port or via an input from said first domain.

35. A processor according to claim 34, said processor comprising a means of blocking write access to said control value via said input port such that setting of said control value can henceforth only be performed by setting said control value via
5 an input from said first domain.

36. A processor according to claim 20, wherein said first domain comprises a first user mode and a first privileged mode and said control value is operable to be set in said storage element via an input from said first privileged mode.

10

37. A processor according to claim 35, wherein said first domain comprises a first user mode and a first privileged mode and said control value is operable to be set in said storage element by input of an authentication code from a mode that is not a first privileged mode followed by an input of said control value.

15

38. A processor according to claim 20, wherein said storage element comprises a register.

39. A processor according to claim 30, wherein said further storage element
20 comprises a register.

25